PASSING FEDERAL SECURITY BREACH LEGISLATION: A "HOW-TO GUIDE"

JOSHUA R. ECKERT*

I. INTRODUCTION

Although large and highly publicized security breaches at Target and Home Depot have recently brought the issue of security breaches to the forefront of the public's attention,[1] federal security breach legislation has been a Congressional priority for the past decade.[2] Despite the federal government's many attempts,[3] however, no such legislation has been passed. In the meantime, security breaches have become increasingly more common. The probability of a company experiencing a large-scale data breach, defined as one containing 10,000 records or greater, has reached 22%.[4] The probability of a similar breach in the United States is slightly lower, though still significant at 18.7%.[5] Further, the risk of falling victim to a security breach is not limited to large corporations.[6] Rather, an increasing number of small businesses and public entities have begun to experience the harm that can be caused by a security breach.[7]

The cost of a security breach upon a company is typically substantial. In addition to the reporting costs imposed by state statutes,[8] the victim of a security breach experiences many more losses that may be more difficult to calculate, such as a loss to the company's

---

* Juris Doctor Candidate, Class of 2016, The Ohio State University Moritz College of Law.

[1] *See* Paul Ziobro & Danny Yadron, *Target Now Says 70 Million People Hit in Data Breach*, WALL ST. J., http://online.wsj.com/articles/SB10001424052702303754404579312232546392464 (last updated Jan. 10, 2014, 8:36 PM); *see also* Press Release, The Home Depot, The Home Depot Reports Findings in Data Breach Investigation (Nov. 6, 2014).

[2] *See* Alina Selyukh, *New Hopes for U.S. Data Breach Law Collide with Old Reality*, REUTERS (Feb. 11, 2014, 3:33 PM), http://www.reuters.com/article/2014/02/11/us-usa-security-congress-idUSBREA1A20O20140211.

[3] *See* Eric Chabrow, *Yet Another Data Breach Bill Introduced*, BANK INFO SECURITY (Feb. 3, 2014), http://www.bankinfosecurity.com/still-another-data-breach-bill-introduced-a-6466/op-1.

[4] PONEMON INST. & IBM, 2014 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 18 (2014).

[5] *Id.* at 19.

[6] *See Resources: Data Breaches by Industry*, CSID, http://www.csid.com/resources/stats/data-breaches-by-industry/ (last visited Apr. 04, 2015) (reporting that educational institutions and governmental agencies experienced a combined 19% of breaches in 2013).

[7] *See id.*

[8] *See* Brian Prince, *Cost of Data Breaches Rises Globally: Report*, SECURITYWEEK (May 5, 2014), http://www.securityweek.com/cost-data-breaches-rises-globally-report (discussing the costs associated with security breach reporting requirements).

reputation.[9] Further, a security breach leads to lost productivity and an increased need for technical support since the company's resources must be diverted to identifying the source of the issue and preventing any further damage.[10] The recent data breach at Target, for example, resulted in a loss of $148,000,000 when all of the costs were taken into account.[11]

In addition, the victim of a security breach may also potentially incur substantial litigation costs arising out of the incident. Home Depot, which experienced a security breach early in 2014, for example, is currently facing twenty-one class action lawsuits related to the breach.[12] Further, financial institutions are increasingly filing suit to recover the costs they incurred in notifying customers and reissuing credit and debit cards after a breach.[13] While such lawsuits may seem desirable in a circumstance where a company has been reckless with the personal information they have obtained, the fact of the matter is that the most expensive of these data breaches are not caused by system glitches or human error but rather by malicious or criminal attacks performed by hackers.[14]

Adding to the cost for companies when they fall victim to a security breach, insurance companies have begun to contest the applicability of their indemnification provisions when one of the companies they cover experiences a security breach.[15] Insurance companies argue that the electronic customer data does not fall within the company's property and that the insurer, therefore, does not need to honor a claim when it is stolen.[16] Further, insurance companies also argue that even if their policies do apply to a security breach, they should not be required to indemnify because the breach likely results from a company violation of consumer financial protection laws.[17] As a result, companies have begun to purchase additional insurance policies

---

[9] *See Data Breach Statistics: An Information Resource for Data Breach Prevention and Response*, IBM, http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/ (last visited Apr. 04, 2015).

[10] *Id.*

[11] *See* Samantha Sharf, *Target Shares Tumble As Retailer Reveals Cost of Data Breach*, FORBES (Aug. 5, 2014, 9:16 AM), http://www.forbes.com/sites/samanthasharf/2014/08/05/target-shares-tumble-as-retailer-reveals-cost-of-data-breach/.

[12] David Allison, *Home Depot Now Facing 21 Class-Action Lawsuits Over Data Breach*, ATLANTA BUS. CHRON. (Oct. 13, 2014, 2:54 PM), http://www.bizjournals.com/atlanta/news/2014/10/13/home-depot-now-facing-21-class-action-lawsuits.html.

[13] *Id.*

[14] PONEMON INST. & IBM, *supra* note 4, at 8.

[15] *See* Amy B. Briggs et al., *Insurer Sues to Prevent Coverage for P.F. Chang's Data Breach*, LEXOLOGY (Nov. 5, 2014), www.lexology.com/library/detail.aspx?g=b83d50d7-71fc-41a9-944e-51440f0518c1&utm_source=Lexology+Daily+Newsfeed&utm_medium.

[16] *Id.*

[17] *Id.*

specifically to cover instances of losses due to a security breach.[18] These additional policies add to the operating costs of the company and represent an additional cost to businesses that is directly attributable to security breaches.

Unfortunately, the technology available to hackers attempting to break into a company's information system has significantly outpaced that which has been available to prevent security breaches.[19] As a result, companies have been limited to a reactive role, attempting to prevent any widespread damages that may occur *after* the breach is discovered. In addition, nearly every state has passed security breach reporting legislation, which attempts to limit the damage caused to customers by requiring companies to report breaches when they do occur.[20]

II. STATE LEGISLATION REPORTING REQUIREMENTS

In an effort to reduce the damage caused to consumers due to data breaches, nearly every state has passed legislation requiring companies that store "personal information" to report security breaches that may have compromised that information.[21] In general, state security breach reporting legislation defines "personal information" as:

> An individual's name or first initial and last name plus one or more of [the] following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes [personal information].[22]

While some states do extend the protections of security breach laws to include personal information recorded in other mediums,[23] these laws generally only apply to electronically held data due to the high risk of that data being accessed maliciously. In addition, several state have expanded the definition of "personal information" to provide greater

---

[18] *See generally* JOSHUA GOLD, ANDERSON KILL & OLICK, P.C., DATA BREACHES AND COMPUTER HACKING: LIABILITY & INSURANCE ISSUES (2011).

[19] Gordon Gibb, *Days After Massive Home Depot Data Breach, Lawsuits Are Filed*, LAWYERSANDSETTLEMENTS.COM (Sep. 16, 2014, 1:45 PM), http://www.lawyersandsettlements.com/articles/data-breach/home-depot-inc-target-eric-w-20100.html#.VHPnPYvF8f2.

[20] *See generally* MINTZ LEVIN, STATE SECURITY BREACH NOTIFICATION LAWS (2015).

[21] *See generally id.*

[22] *Id.* at 1.

[23] *E.g.*, *id.* at 15 (detailing Indiana's data breach legislation).

protection to consumers.[24] These expanded definitions of "personal information" often include items such as Social Security numbers *standing alone*, medical information, insurance information, biometric data, and usernames or e-mails in conjunction with a password, which could provide access to an online account.[25]

Although the definition of "personal information" can be expansive in some states, reporting requirements are not always triggered when such information has been accessed. Most states include an exception for data that is encrypted.[26] In addition, several states limit the reporting requirement trigger to only events that have, are reasonably believed to, or are substantially likely to lead to the identity theft of the affected consumers.[27] Further, a large portion of state security breach reporting legislation excludes individuals and government agencies from the reporting requirements.[28]

While reporting requirements are not always triggered by an unauthorized access to "personal information," the reporting requirements placed on covered entities that do experience a security breach are substantial once they are triggered. When a triggering event occurs, most states require that all individuals who might have been affected by the breach be notified.[29] In some states, however, notifying only those individuals who might have been affected is still insufficient.[30] Twelve states require that the company notify the state attorney general depending on the number of people affected.[31] Some states also require companies to notify credit reporting agencies and occasionally even the state police when a breach occurs.[32]

State security breach reporting requirements also differ slightly as to the methods by which notification can be given. Most states allow for notifications to be sent by either mail or e-mail.[33] States that allow notification to be sent by e-mail, however, often also require that the company first receive permission from the customer to receive such notifications in that manner.[34] Further, in several states, it is not enough for the customer to simply contractually agree to receive such notifications by e-mail as part of a boilerplate agreement; the permission

---

[24] *Id.*
[25] *Id.*
[26] *See* BAKER & HOSTETLER LLP, DATA BREACH CHARTS 15–18 (2014).
[27] *See generally* MINTZ LEVIN, *supra* note 20.
[28] *See generally id.*
[29] *See generally id.*
[30] *See* Reid J. Schar & Kathleen W. Gibbons, *Complicated Compliance: State Data Breach Notification Laws*, BLOOMBERG LAW (Aug. 09, 2013), http://www.bna.com/complicated-compliance-state-data-breach-notification-laws/.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*

must be given with the customer fully aware of all rights under the statute.[35] In addition to mail and e-mail, all states, with the exception of Utah, allow for a substitute method of notice to be used that otherwise complies with the statute.[36] These substitute methods, however, are often not made available to companies unless it can be proven that utilizing the standard notification methods would cost more than a standard threshold amount (ranging from $5,000 on the low end to $250,000 on the high end).[37] Substitute methods of notification can also be utilized in some states as long as the company can demonstrate that a threshold number of individuals must be notified.[38]

State reporting requirement statutes also differ substantially in the content that must be included in the notification and the time limits allowed for notification. While some statutes do not have any specific content requirements, others extensively prescribe the content that must be included.[39] California's statute, for example, requires:

> (a) [T]he name and contact information of the company; (b) the types of personal information subject to the breach; (c) the date of the breach (actual, estimate, or range); (d) whether notice was delayed for a law enforcement investigation; (e) a general description of the incident; and, under certain circumstances, (f) contact information for the major credit reporting agencies.[40]

State statutes also vary drastically in relation to the time limits allowed for notification. Most statutes do not set a specific time limit for notification, requiring only that companies provide the notification "in the most expedient time possible" or "without unreasonable delay."[41] Some states, on the other hand, provide very specific time limits for reporting to customers.[42] In addition, all states allow for notification to be delayed for the purpose of investigation into the breach by law enforcement.[43] Further, the reporting requirements may differ depending on whether the company owns the data that has been obtained. In many states, those who do not own the data must notify the owner immediately once a breach has been discovered.[44]

State statutes also differ on the remedies available when a company

---

[35] *Id.*
[36] Schar & Gibbons, *supra* n. 30.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] Schar & Gibbons, *supra* n. 30.
[43] *Id.*
[44] *Id.*

has not complied with notification requirements. While some statutes merely set a maximum civil penalty per breach, others calculate penalties based upon the size of the breach or the number of days the company was non-compliant with the statute.[45] In addition, ten states currently offer a private right of action to citizens who have been affected by a security breach.[46] The availability of a private right of action has led to companies facing multiple lawsuits based on a single security breach incident, and it has also led to an increase in class-action lawsuits alleging non-compliance with security breach notification regulations.[47]

In addition to security breach reporting requirements, several states are beginning to add additional protections for consumers. Several states have enacted complementary provisions to their security breach notification laws, which require that companies maintain adequate policies to protect against security breaches.[48] California, however, has taken an additional step, which is yet to have been done by any other state. In a recent amendment to their state breach notification law, California added a requirement that companies *must* offer to provide identity theft and mitigation services.[49] While making such an offer has been a common practice amongst companies that have experienced a security breach, California is the first state to require that identity theft and mitigation services be offered.[50]

III. 2014: INCREASING STATE SECURITY BREACH LEGISLATION

The year 2014 saw a dramatic increase in states' regulation of security breaches, with twenty-three states considering some form of security breach legislation.[51] Of these twenty-three states, eleven enacted some form of security breach legislation for businesses, education institutions, or government entities, usually through amendment.[52] In addition to those states that added to or clarified their security breach notification laws, Kentucky enacted its first laws regarding security breach notification, making forty-seven states that

---

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *See generally* MINTZ LEVIN, *supra* note 20.
[49] Tanya Forsheit & M. Scott Koller, *California's Latest Amendments to Its Data Security Breach Notification Law – Much Ado about Nothing?*, BAKER & HOSTETLER LLP (Oct. 02, 2014), http://www.bakerlaw.com/alerts/californias-latest-amendments-to-its-data-security-breach-notification-law-much-ado-about-nothing.
[50] *Id.*
[51] *2014 Security Breach Legislation*, NAT'L CONF. ST. LEGISLATURES (Dec. 23, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/2014-security-breach-legislation.aspx.
[52] *Id.*

now have some form of security breach regulations.[53] The willingness of these state legislatures to continue increasing protections for consumers, as they relate to security breaches, indicates not only an increasing need for these protections, but also a belief that it is unlikely that comprehensive federal security breach legislation will be passed in the near future. Below are several examples of new protections afforded to consumers under security breach laws passed in eleven states this year.

A. California

California passed perhaps the most comprehensive set of security breach amendments in 2014. In addition to requiring companies to maintain security procedures for the protection of their customers' personal information, the state now requires any entity that has experienced a security breach to offer identity theft protection services to affected individuals for at least twelve months at the company's expense.[54] Further, California increased the reporting requirements for clinics, health facilities, home health agencies, and hospice organizations when they experience a security breach.[55]

B. Kansas

In 2014, the state of Kansas expanded its security breach notification requirements by passing legislation that relates to the personal information of students that is collected by schools. The new law requires that "in the event of a security breach by any educator entity or third party given access, the parent or legal guardian of each affected student shall be immediately notified of the breach."[56] Although the law does provide enhanced protections to students, it would not appear to apply to malicious attacks by outside parties.[57]

C. Minnesota

Much like California, Minnesota also passed comprehensive security breach reform in 2014, specifically as it relates to the unauthorized access of data by public employees.[58] Minnesota law now requires that procedures be put in place to guarantee that personal information is only available to public employees whose work

---

[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *2014 Security Breach Legislation*, *supra* n. 51.
[57] *Id.*
[58] *Id.*

assignment reasonably requires the data.[59] It also now requires that written notification be given to affected persons when such a breach occurs and provides criminal penalties for individuals who knowingly authorize improper access to personal information.[60]

D. South Carolina

South Carolina expanded protections for its citizens and their personal information in 2014 by passing security breach legislation requiring state agencies to develop and maintain cyber-security policies and guidelines.[61] The state gave authority to the Division of State Technology to perform audits on most state agencies to ensure they are following these newly enacted policies and guidelines.[62] In addition, the state gave the Division of State Technology the authority to investigate and respond to any security breaches that might occur within the state's agencies.[63]

E. Vermont

Vermont took security breach legislation an additional step in 2014 by placing affirmative responsibilities upon state law enforcement agencies when they have a reasonable belief that a security breach either has or may have occurred at a specific business.[64] Upon attaining a reasonable belief, the law enforcement agency must notify the specific business in writing and notify the business that additional information may need to be provided to the Vermont Office of the Attorney General or the Vermont Department of Financial Regulation.[65] Placing an affirmative obligation upon law enforcement agencies to notify businesses that they believe have experienced a security breach is a new concept that seems to demonstrate Vermont's dedication to protecting its consumers.

IV. PROS AND CONS OF FEDERAL SECURITY BREACH LEGISLATION

The complicated and patchwork nature of state security breach laws has made it incredibly difficult for companies to guarantee compliance when a breach has occurred. As a result, many have been

---

[59] *Id.*
[60] *Id.*
[61] *2014 Security Breach Legislation, supra* n. 51.
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*

pushing for federal security breach legislation.[66] Such legislation would preempt the current state statutory schemes and would simplify compliance efforts for companies that have been affected by a security breach.[67] In turn, the cost for companies that have experienced a security breach would decrease. Further, despite industry arguments to the contrary, a single federal security breach law would enhance the ability of law enforcement to investigate those who are causing the security breaches.[68] According to United States Attorney General Eric Holder, such a law would "enable law enforcement to better investigate these crimes -- and hold compromised entities accountable when they fail to keep sensitive information safe."[69]

In addition to the reduced cost to companies and an increased ability to investigate security breaches, a single federal security breach law would encourage equality amongst consumers across the country. The current state regulatory system provides consumers with different protections depending upon the state in which they reside.[70] Such a result, however, runs contrary to the general sentiment felt amongst consumers and expressed by Eva Velasquez, chief executive of San Diego-based non-profit Identity Theft Resource Center, that "[y]ou shouldn't have more or less protection because of the state you reside in."[71]

While there are many positives to passing federal security breach regulations, consumer advocacy groups point out that there are several concerns as well. First and foremost, consumer advocates are concerned that passing any federal security breach legislation would remove protections that are currently available to consumers under some of the more stringent state codes.[72] As a solution, consumer advocates have pushed for federal legislation that would serve as a floor upon which state codes could build.[73] This position is also supported by many state legislatures, according to the National Conference of State Legislatures' committee director for state-federal relations, James Ward.[74]

Although the introduction of a federal security breach law as a minimum standard would greatly increase consumer protections, it

---

[66] *See* Danielle Douglas, *Here's Why the Government Wants a National Data Breach Law*, WASH. POST (Feb. 24, 2014), http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/24/heres-why-the-government-wants-a-national-data-breach-law/.
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *See* Tod Newcombe, *States Approach Federal Data Breach Law With Caution*, GOVERNING THE STS. & LOCALITIES (Oct. 2014), http://www.governing.com/columns/tech-talk/gov-federal-cybersecurity-law.html.
[73] *Id.*
[74] *Id.*

would also undermine the goal of federal legislation. Currently, companies that experience a security breach must comply with different reporting requirements in nearly every state in the country.[75] If the federal standard were to serve only as a baseline for state security breach standards, companies that experience a security breach would still be required to comply with all of the state standards over and above the federal baseline. In essence, a federal security breach law that operates only as a minimum standard would add another piece to the patchwork that is security breach notification law instead of eliminating the difficulties associated with having such a complex scheme.[76]

V. PENDING FEDERAL LEGISLATION

Congress' most recent attempt at passing comprehensive federal security breach legislation, entitled the Data Security and Breach Notification Act of 2014 ("the Act"), was introduced in the Senate on January 30, 2014.[77] Procedurally, the bill has been a non-starter, seemingly having been killed in the Committee on Commerce, Science, and Transportation.[78] The text of the bill, however, provides insight into why Congress has had such a difficult time passing federal security breach legislation.

Unlike many state security breach statutes, the Data Security and Breach Notification Act of 2014 contains both proactive and reactive measures designed to protect consumers from the harm caused by security breaches.[79] The proactive measures instituted by the Act require that companies adopt "general security policies and procedures" to protect against the unauthorized access of "personal information."[80] While the Act does lay out some of the requirements for "policies and procedures,"[81] the Federal Trade Commission ("FTC") determines what constitutes these based on factors such as the size, nature, and scope of business performed by the covered entity, the current state of technology available in protecting against security threats, the costs of implementing safeguards, and the impact the implementation of these policies will have on small business and non-profit organizations.[82]

Further, the Act imposes civil penalties upon covered entities that fail to implement reasonable policies in accordance with the regulations

---

[75] *See* Selyukh, *supra* note 2.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014).
[80] *Id.* § 2(a)(1).
[81] *Id.* § 2(a)(2).
[82] *Id.* § 2(a)(1)(A)–(D).

promulgated by the FTC.[83] When a company is deemed non-compliant with this section, it is liable for up to $11,000 per violation for each day it has been non-compliant.[84] Notwithstanding the number of actions being brought against the company under this section, the maximum penalty is capped at $5,000,000 per violation.[85]

Unlike the proactive provisions laid out in the Act, the reactive, or reporting, requirements are fairly similar to the requirements imposed by may state security breach statutes. "Personal information," which is protected by the Act, includes:

> (i) [A] non-truncated social security number; (ii) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction; or (iii) an individual's first and last name or first initial and last name in combination with-- (I) a driver's license number, a passport number, or an alien registration number, or other similar number issued on a government document used to verify identity; (II) unique biometric data such as a finger print, voice print, retina or iris image, or any other physical representation; (III) a unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value; or (IV) 2 of the following: (aa) Home address or telephone number. (bb) Mother's maiden name, if identified as such. (cc) Month, date, and year of birth.[86]

In addition, there is a provision that allows the FTC to alter the definition of "personal information" under the Act if the provided definition is not "reasonably sufficient to protect individuals from identity theft, fraud, or other unlawful conduct."[87]

Similar to many state statutes, the Act would require notification to customers whose personal information "was or is reasonably believed to have been acquired or accessed" due to the breach.[88] An exception is granted, however, as in most state statutes, when a company concludes that there is "no reasonable risk of identity theft, fraud, or other unlawful

---

[83] *Id.* § 5(d)(2).
[84] *Id.* § 5(d)(2)(A)(i).
[85] Data Security and Breach Notification Act of 2014, at § 5(d)(2)(C)(i)
[86] *Id.* § 6(9)(A)(i)–(iii)(IV)(cc).
[87] *Id.* § 6(9)(B).
[88] *Id.* § 3(a)(1).

conduct" resulting from the breach.[89] The Act further insulates companies that experience a breach by creating a rebuttable presumption that acquisition of information which has been rendered unusable or unreadable by virtue of security measures, such as encryption, does not constitute a "reasonable risk of identity theft, fraud, or other unlawful conduct."[90]

Once the notification requirement has been triggered, the Act provides many of the same alternatives available to companies under state statutes for the form the notification may take. Like all state statutes, the notification may come in the form of mail or e-mail, provided that the company has received permission to send such a notification by e-mail from the customer.[91] In addition, substitute methods of notification, specifically over e-mail, web posting, or print or broadcast media, are available if the company can show that it maintains less than 10,000 records and that notification through standard means is infeasible due to excessive cost.[92]

Unlike many state security breach statutes, the content requirements of the notification are explicitly prescribed within the Act. Similar to California's statute, the Act would require the notification to contain the date of the breach, a description of the information that is believed to have been obtained, and contact information for the company.[93] In addition, however, the individual must be informed of the potential right to a consumer credit report, how to go about getting a consumer credit report, how to contact major credit agencies, and how to access information on the FTC's page regarding identity theft.[94]

The proposed Act is also very explicit regarding the time limits for compliance with the reporting requirement. Unlike many states which require only that notification be given "in the most expedient time possible" or "without unreasonable delay," the Act sets a time limit, specifically thirty days, for the notification of customers once a security breach has been discovered.[95] Exceptions are granted, however, if it can be shown that providing notice within the timeframe is not feasible due to circumstances necessary to identify affected customers, to prevent further breach, or to reasonably restore the integrity of the data.[96] Further, instead of leaving it to the company's discretion to delay notification due to investigations by law enforcement like most state statutes, the Act imposes an affirmative duty on the company to report

---

[89] *Id.* § 3(g)(1).
[90] *Id.* § 3(g)(2)(A)–(B).
[91] Data Security and Breach Notification Act of 2014, at § 3(d)(i)(I)–(II)(bb).
[92] *Id.* § 3(2)(A)–(B).
[93] *Id.* § 3(d)(B)(i)–(iii).
[94] *Id.* § 3(d)(B)(iv)–(vii).
[95] *Id.* § 3(c)(1).
[96] *Id.* § 3(c)(2)(A)–(C).

any breaches to law enforcement.[97] Notification will only be delayed if permission is received by the law enforcement agency to delay notification pending the investigation.[98]

Similarly to the proactive provisions, the Act also imposes civil penalties upon companies that fail to comply with either the customer or law enforcement notification requirements. Failure to comply with the customer reporting requirements results in a penalty up to $11,000 per violation,[99] capped at $5,000,000 for each incident of breach.[100] Failure to comply with law enforcement notification requirements results in a penalty of up to $1,000 per individual whose information was stolen capped at $100,000 per day in non-compliance.[101] Such penalties are further limited to $1,000,000 per security breach incident unless the non-compliance is found to be willful or intentional, which results in an additional $1,000,000 penalty.[102]

One area in which the proposed Act provides greater certainty than most state statutes is regarding who may bring an action for damages resulting from violations of the Act. The proposed Act rejects a private right of action in favor of a dual enforcement approach. The Act would give each individual state's attorney general the authority to bring an action for violation of any of the above responsibilities on behalf of citizens of the state.[103] Before asserting this authority, however, the attorney general would be required to give notice to the FTC, which would have a right to intervene in the action and gain complete control of the case.[104]

Finally, and probably most importantly, the Act is designed to preempt state security breach legislation for those entities that are covered. The Act states that for covered entities, it supersedes any state law that requires security practices regarding the treatment of personal information or any state law that deals with the notification of individuals in the event of a security breach.[105] Further, the Act would preempt any individual who is not otherwise stated in the Act from bringing a civil action "if such action is premised in whole or in part upon the defendant violating any provision of this Act."[106] In the end, the only function reserved for the states as it relates to security breach law under this Act would be for circumstances constituting fraud or that

---

[97] Data Security and Breach Notification Act of 2014, at § 4(b).
[98] *Id.* § 3(h).
[99] *Id.* § 5(d)(2)(A)(ii).
[100] *Id.* § 5(d)(2)(C)(ii).
[101] *Id.* § 5(e)(2)(A).
[102] *Id.* § 5(e)(2)(B).
[103] Data Security and Breach Notification Act of 2014, at § 5(d)(1), 5(e)(1)
[104] *Id.* § 5(d)(3)(A)(i)–(iii).
[105] *Id.* § 7(a)(1)–(2).
[106] *Id.* § 7(b)(1).

would fall under trespass, contract, or tort law.[107]

VI. CRITIQUE OF THE DATA SECURITY AND BREACH NOTIFICATION ACT OF 2014

The primary issue with the Data Security and Breach Notification Act of 2014 is that its regulations are simultaneously too broad and too narrow, drawing opposition from companies and consumer advocacy groups alike. First and foremost, the potential penalties for violations under the proactive provisions of the Act are excessive and unnecessary. As discussed above, companies that experience a data breach already suffer a substantial financial burden under the current regime.[108] In addition, the non-monetary costs, such as loss of productivity and reputational harm, provide further incentives for companies to strive to protect their customers' "personal information."[109] The inclusion of these proactive measures, therefore, seems somewhat unnecessary given the incentives that already exist for companies to adequately protect their data.

Further, the penalty scheme as it relates to the proactive measures is extreme considering that in reality there is little that a company can do to guarantee the protection of information. The largest and most costly security breaches that have occurred have been the result of malicious or criminal hackers[110] and, unfortunately, the technology available to hackers has continually outpaced that which is available to companies for security purposes.[111] Even still, the penalty scheme under the proactive provisions contemplates nearly unlimited liability for those companies that fall victim to these attacks. Under the proactive provisions of the Act, the FTC has been given the power to dictate what constitute reasonable policies.[112] For each instance where a company's policies do not line up with what the FTC determines to be a reasonable policy, the FTC may seek a penalty of up to $11,000.[113] Further, this $11,000 would continue to multiply by the number of days the company's policy was inconsistent with reasonable policies.[114] What makes a company's liability truly unlimited, however, is that penalties are capped at $5,000,000 for *each* violation, not each time its policies

---

[107] *Id.* § 7(c).
[108] *See generally* PONEMON INST. & IBM, *supra* note 4.
[109] *Id.*
[110] *Id.*
[111] *See* Gibb, *supra* note 19.
[112] Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. § 2(a)(1) (2014).
[113] *Id.* § 5(d)(2)(A)(i).
[114] *Id.*

fall out of line with reasonable policies as a whole.[115] A company, therefore, could potentially face unlimited liability for failing to have reasonable policies according to the FTC once a security breach has been discovered and the FTC retroactively looks at the company's security policies with the benefit of hindsight.

While the problems with the proactive provisions of the Act are troubling to companies, there are several deficiencies with the reporting requirements that are equally troubling to consumer advocate groups on the other side. First and foremost, the Act's reporting requirements, while clear and arguably fair, are not nearly as stringent as some states' security breach reporting laws. For example, the exclusion of certain types of data, such as medical or insurance information, from the definition of "personal information" might leave information that otherwise would have been protected by state statutes unprotected.[116] Further, allowing a company to unilaterally make a determination that the security breach does not pose a substantial risk of identity theft is outside the realm of what is contemplated by most state statutes.[117]

In addition, the inclusion of an "opt-in" provision[118] and preemption clause[119] effectively eliminates any role that the states might play in the protection of their citizens' personal information. Although the statute does not cover public agencies, such agencies and several other types of entities are allowed to opt-in to coverage under the federal statute. Ultimately, entities will opt-in to the federal provisions, even if not initially subject to them, whenever their states' standards are more stringent than the federal standard. Further, the preemption clause will also make the proactive provisions of state statutes, some of which are even more stringent than the federal statute, inoperable as protections for citizens of that state.

VII. SECURITY BREACH LEGISLATION IN THE STATE OF THE UNION ADDRESS

Cyber-security and federal security breach legislation once again captured the nation's attention after President Barack Obama publicly introduced his proposal for a federal security breach law during the 2015 State of the Union Address.[120] During his speech, the President urged Congress to commit to a bi-partisan effort "to finally pass the legislation

---

[115] *Id.* § 5(d)(2)(C)(i).
[116] *See generally id.* § 6(9).
[117] *Id.* § 3(g)(1).
[118] *Id.* § 5(b).
[119] *Id.* § 7(a).
[120] *See* Ezra D. Church et al., *Proposed Data Breach Legislation Announced*, NAT'L L. REV. (Jan. 23, 2015), http://www.natlawreview.com/article/proposed-data-breach-legislation-announced.

we need to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information."[121] The need for comprehensive federal security breach legislation and reform has become increasingly apparent due to the highly publicized cyber-attacks on two large American companies, Staples[122] and Sony.[123] The security breach at Staples affected 115 stores nationwide and caused an estimated 1,160,000 credit and debit cards to become susceptible to identity theft.[124] While the security breach at Sony Pictures did not have such a quantifiable effect on consumers, it did cause the film studio to pull the nationwide launch of a major motion picture and made headlines due to the alleged perpetrator, the North Korean government.[125]

While the President did not elaborate on the contents of any such federal security breach legislation during his State of the Union Address, he did discuss details regarding his proposal for legislation at a speech given to the Federal Trade Commission a little over a week earlier.[126] During this speech, the President highlighted that a single federal security breach law would be beneficial to both businesses and consumers due to the increased clarity it would provide stating, "right now almost every state has a different law on this and it's confusing for consumers and it's confusing for companies — and it's costly too, to have to comply with a patchwork of laws."[127] The White House has since released the full text of the proposed legislation that President Obama discussed with the Federal Trade Commission and alluded to in the State of the Union Address.[128]

While the bill proposed by President Obama is similar in many respects to several state security breach notification laws and previous federal legislation that has been proposed in the area, there are several

---

[121] Barack Obama, President of the United States, State of the Union Address (Jan. 20, 2015).

[122] *See* Whit Richardson, *Staples Says Customers of Maine Stores Affected by Data Breach Should Check Accounts*, PORTLAND PRESS HERALD (Jan. 12, 2015), http://www.pressherald.com/2015/01/12/staples-data-breach-affects-two-of-its-stores-in-maine/.

[123] *See* Dave Lewis, *Sony Pictures Data Breach and the PR Nightmare*, FORBES (Dec. 16, 2014, 3:00 AM), http://www.forbes.com/sites/davelewis/2014/12/16/sony-pictures-data-breach-and-the-pr-nightmare/.

[124] *See* Richardson, *supra* note 115.

[125] *See* Martyn Williams, *FBI Concludes North Korea Was 'Responsible' for Sony Hack*, COMPUTERWORLD (Dec. 19, 2014, 12:27 PM), http://www.computerworld.com/article/2861460/fbi-concludes-north-korea-was-responsible-for-sony-hack.html.

[126] *See* Louis S. Dennig, IV, *President Obama Proposes Strict National Data Breach Notification Law Ahead of State of the Union*, LEXOLOGY (Jan. 19, 2015), http://www.lexology.com/library/detail.aspx?g=ab2d1f4b-e41f-47ab-9915-da0642882dfc.

[127] *Id.*

[128] *Id.*; *see also* Personal Data Notification & Protection Act (2015) (proposed by President Barack Obama)

key differences. First and foremost, the proposed bill broadens the definition of "personal information" in comparison to previous versions of proposed federal security breach legislation and current state security breach notification laws.[129] Unlike state laws, the proposed bill would trigger notification requirements when certain pieces of information were obtained standing alone, without reference to an individual's name or identification.[130] Such pieces of information include credit or debit card numbers, complete social security numbers, driver's license numbers, passport numbers, alien registration numbers, biometric data, and an email or username in combination with a password.[131] In an additional split from some states' security breach notification laws, the proposed bill would also trigger notification requirements not only when "personal information" is acquired, but also whenever there is unauthorized access to such information.[132]

While the above differences are noteworthy, most of the remainder of the proposed legislation is fairly similar to the Data Security and Breach Notification Act of 2014. The proposed legislation would require the notification[133] within thirty days[134] to individuals who have had their "sensitive personally identifiable information" acquired.[135] Businesses comply with these requirements by providing direct notification through mail, individual telephone notification, or e-mail notification, in conjunction with mass media notification.[136] In addition to individuals, the proposed bill would also require notification to major consumer reporting agencies under certain conditions,[137] as well as notification to law enforcement and national security agencies.[138] Further, the proposed legislation would give dual authority to each state's attorney general as well as the Federal Trade Commission to take action on behalf of citizens for violations of the law.[139] Finally, the proposed legislation contains a preemption clause which would make the law "supersede any provision of the law of any State, or political subdivision thereof, relating to notification of a business entity engaged in interstate commerce of a security breach of computerized data, except as provided in section 104(c)."[140] The referenced section in the preemption clause provides that a state may require notifications to "include information

---

[129] *See* Dennig, *supra* note 119.
[130] *Id.*
[131] *Id.*
[132] *Id.*
[133] Personal Data Notification & Protection Act § 101(a).
[134] *Id.* § 101(c)(1)–(2).
[135] *Id.* § 1(h).
[136] *Id.* § 103.
[137] *Id.* § 105.
[138] *Id.* § 106.
[139] Personal Data Notification & Protection Act, at §§ 107–08.
[140] *Id.* § 109.

regarding victim protection assistance provided for by that State."[141]

Notably missing from the President's proposed federal security breach legislation are proactive measures that require a company to maintain data protection standards to protect consumers' "sensitive personally identifiable information."[142] Such measures have been a focal point of previous federal security breach legislation, especially the Data Security and Breach Notification Act of 2014.[143] Presumably, such proactive measures requiring a company to maintain data protections standards would still be governed by state security breach laws. In addition, the proposed legislation does not detail the damages that the Federal Trade Commission or states' attorneys general may seek to obtain through civil action on behalf of their citizens. Ultimately, this will likely be an issue left up to Congress or promulgated by the Federal Trade Commission. Finally, it is important to note that the proposed legislation would not require companies to provide credit-monitoring services upon a triggering event, as most people have interpreted the Data Security and Breach Notification Act of 2014 to require.[144]

VIII. CRITIQUE OF THE PERSONAL DATA NOTIFICATION AND PROTECTION ACT

Many media outlets and legal experts have weighed in on the potential effectiveness of the President's proposed federal security breach legislation since it was first introduced in his recent speeches to the Federal Trade Commission and the State of the Union Address.[145] While some believe that the proposed legislation is a stringent set of rules, which will represent an increase in protection for consumers,[146] others are quick to point out deficiencies within the proposed legislation.[147] In general, companies that have a national presence have tended to comply with the strictest of the states' data breach notification laws to simplify compliance procedures.[148] Therefore, in areas of the proposed legislation where less protection is provided to consumers, it will have the effect of harming all consumers across the country and not

---

[141] *Id.* § 104(c).
[142] *Id.* § 1(h).
[143] Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. § 2(a)(1) (2014).
[144] *Id.* § 3(d)(B)(iv)–(vii).
[145] *See, e.g.*, Dennig, *supra* note 119.
[146] *See id.*
[147] *See* G.S. Hans, *White House Data Breach Legislation Must be Augmented to Improve Consumer Protection*, CENTER FOR DEMOCRACY & TECH. (Jan. 16, 2015), https://cdt.org/blog/white-house-data-breach-legislation-must-be-augmented-to-improve-consumer-protection/.
[148] *Id.*

just those in the states with the strictest data breach notification laws.[149] For example, the proposed legislation would require notification of individuals without unreasonable delay within a time period that cannot exceed thirty days.[150] Since, however, there are states that would require a more timely notification, the proposed legislation would likely mean an overall decrease in the timeliness of notification for all consumers across the nation.[151]

In addition, there is concern that the proposed legislation will not do enough to help protect consumers' information in the first place. Unlike the Data Security and Breach Notification Act of 2014, the legislation proposed by the President does not require that any proactive measures be taken by companies to secure consumers' personal information.[152] The lack of these kinds of requirements has some organizations concerned that there will not be enough of an incentive for companies to develop significant and effective procedures to help protect the personal information that they store.[153] Further, financial industry trade groups have begun pushing for increased security requirements for retailers to help protect consumers' personal information.[154] Companies in the financial industry must already comply with a robust set of protection procedures when it comes to securing their clients' personal information and are often saddled with the costs of fraudulent transactions when retailers experience security breaches due to their lack of protection procedures.[155] Because of this, members of the financial industry have not only been calling for increased security requirements for retailers, but have also been demanding that retailers help pay the costs these financial institutions incur due to these breaches.[156]

Ultimately, the federal security breach legislation proposed by the President has many of the same strengths and weaknesses as previous federal security breach legislative proposals. Much like the Data Security and Breach Notification Act of 2014, the President's proposed legislation has received criticism as being an actual decrease in protection for consumers. While the proposed bill's definition of

---

[149] *Id.*

[150] Personal Data Notification & Protection Act § 101(c) (2015) (proposed by President Barack Obama).

[151] Hans, *supra* note 140.

[152] *Id.*

[153] *Id.*

[154] *See* Evan Weinberger, *Financial Trade Groups Push Congress for Data Breach Law*, LAW360 (Jan. 23, 2015, 5:22 PM), http://www.law360.com/retail/articles/614693/financial-trade-groups-push-congress-for-data-breach-law.

[155] *Id.*

[156] *See* Evan Weinberger, *OCC Chief Says Retailers Must Bear Some Data Breach Costs*, LAW360 (Nov. 07, 2014, 1:52 PM), http://www.law360.com/articles/594409/occ-chief-says-retailers-must-bear-some-data-breach-costs.

"sensitive personally identifiable information" does increase the number of notification triggers to some extent, there are also some types of data which are currently protected by state security breach notification laws that will lose protection due to preemption, such as certain state laws involving health data.[157] Because the proposed legislation would in effect decrease the level of protection available under state security breach notification laws, it is likely that it will continue to see strong opposition from consumer advocacy groups in its current form.

There are, however, several positive aspects of the President's proposed legislation that are worth mentioning. As discussed above, the inclusion of proactive measures requiring companies to implement security procedures is unnecessary given that companies already face substantial costs whenever they fall victim to a security breach.[158] Further, while some companies are making strides toward preventing identity theft through security breaches,[159] the technology available to companies to prevent security breaches in the first place currently lags behind the technology available to hackers.[160] In removing these proactive measures from the proposed bill, the government has recognized that sufficient incentives to prevent security breaches already exist under the notification regime and also leave room for state legislation in the area if the states wish to add additional protections for their consumers.

Most importantly, the Personal Data Notification & Protection Act proposed by President Obama includes reporting requirements to law enforcement and national security agencies. In doing so, the bill would place emphasis on protecting consumers from hackers by making sure that they are caught and prosecuted. As President Obama put it in his speech to the Federal Trade Commission, the goal of the legislation is to "close loopholes in the law so we can go after more criminals who steal and sell the identities of Americans — even when they do it overseas."[161] This goal is an important one to strive to achieve and, according to President Obama, "should be something that unites all of us as Americans."[162]

---

[157] *See* Alicia Gilleskie, *What Obama's Proposed Anti-Hacking Legislation Means for Entrepreneurs*, ENTREPRENEUR (Jan. 23, 2015), http://www.entrepreneur.com/article/242099.

[158] *See* PONEMON INST. & IBM, *supra* note 4.

[159] *See* Jennifer Van Grove, *MasterCard Announces A Credit Card Even A Security Fanatic Can Love*, THESTREET (Jan. 07, 2015, 5:13 PM), http://www.thestreet.com/story/13003518/1/mastercard-announces-a-credit-card-even-a-security-fanatic-can-love.html.

[160] *See* Gibb, *supra* note 19.

[161] Maria Korolov, *Obama Proposes New 30-Day Data Breach Notification Law*, CSO (Jan. 13, 2015, 11:55 AM), http://www.csoonline.com/article/2868096/data-protection/obama-proposes-new-30-day-data-breach-notification-law.html.

[162] *Id.*

IX. RECOMMENDATIONS FOR EFFECTIVE FEDERAL SECURITY BREACH LEGISLATION

While nearly everyone agrees that comprehensive federal security breach legislation would be beneficial, Congress has been unable to pass any such legislation for a decade.[163] The reason for this is that none of the bills that have been introduced have adequately addressed the concerns of businesses, state legislatures, and consumer advocacy groups. Businesses, while welcoming the simplicity of a single federal regulatory scheme, will reject such a scheme if it imposes burdens that are above and beyond those that are implemented by most states. State legislatures and consumer advocacy groups, on the other hand, while recognizing the equality amongst consumers that would exist under a federal regulatory scheme, will be skeptical of any federal legislation that is not at least as protective of their citizens as their current state statutory scheme. Fortunately, there is common ground that can be found and compromises that can be made to help facilitate the passing of an effective federal security breach law.

First and foremost, significant consideration needs to be given to the proactive provisions of the bill, which impose penalties upon companies for failure to keep "reasonable security procedures." Without prior knowledge of what the FTC is going to consider a "reasonable security procedure," such provisions will continue to be a substantial roadblock for businesses when it comes to federal security breach legislation. As discussed above, numerous incentives already exist for companies to maintain adequate security procedures to protect their customers' "personal information." Target, for example, experienced losses totaling $148,000,000 due to its recent security breach.[164] Clearly, a sufficient incentive already exists for companies to attempt to protect their customers' "personal information" as much as possible.

Also to be taken into consideration is the fact that companies do not have the tools available to them to prevent the most significant and expensive of these breaches. The technology available to hackers substantially outpaces the tools available to businesses to protect their information systems.[165] What this means, unfortunately, is that security breaches are inevitable no matter what security policies a company may implement. Imposing almost unlimited liability upon companies that are essentially the victims of inevitable malicious and criminal attacks is hard to justify considering that adequate incentives already exist for companies to maintain the strongest security policies possible to protect

---

[163] *See* Press Release, Dianne Feinstein, Senator, U.S. Cong., Senators Introduce Bill to Protect Against Data Breaches (Jan. 30, 2014).
[164] *See* Sharf, *supra* note 11.
[165] *See* Gibb, *supra* note 19.

their customer's "personal information." The inclusion, therefore, of harsh penalty provisions related to the proactive provisions of a bill[166] will likely draw stark opposition from businesses.

On the other side of the table, reporting requirements need to be at least as stringent as the strictest states' security breach laws to draw support from state legislatures and consumer advocacy groups. In relation to the Data Security and Breach Notification Law of 2014, this means that several changes would need to be made to the reporting requirements. First, the definition of "personal information" would need to be expanded to encompass different types of personal information that are covered by some state statutes. Second, although the Act's reporting requirements are fairly strict once they are triggered, the exception that allows the company to avoid notification once a determination has been made that no significant risk of identity theft exists is a substantially broader exception than is provided by most states. Third, the Act would need to expand covered entities to include all entities that are included in some states' security breach statutes, such as governmental agencies. In short, by increasing the stringency of the federal regulation and those that are covered by it, the statute will gain more support from state legislatures and consumer advocacy groups.

As a counter to the increased stringency and coverage of the federal regulation, Congress might also wish to include an "opt-out" provision. An opt-out provision would allow entities to remove themselves from being covered by the federal regulation and instead continue to be covered under the current state scheme. This would require entities to perform an opportunity cost analysis, weighing the benefits of the simplicity of a federal regulatory scheme against the less stringent standards offered by some states. For small businesses that operate in only a few states, this may be a more attractive option considering they might not be covered by stringent reporting standards in those states.

Additionally, the inclusion of an opt-out provision may adequately address the concerns that some businesses may have regarding any proactive provisions in the bill. Most state security breach laws are entirely reactive and do not impose penalties upon an entity for failing to adequately protect data.[167] As such, some businesses may wish to opt-out of the federal regulation to avoid those types of requirements if they primarily operate in states that do not have similar provisions.

An opt-out provision stands in stark contrast to the "opt-in" provision proposed in the Data Security and Breach Notification Act of 2014. The opt-in provision contemplated that some entities would wish to escape the stringent notification requirements of their state security

---

[166] Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. § 5(d)(2)(C) (2014).

[167] *See generally* MINTZ LEVIN, *supra* note 20.

breach laws by opting to be covered by federal legislation instead. An opt-out provision, on the other hand, represents an opportunity for entities to perform a cost-benefit analysis regarding the federal regulations and still gives state legislatures the opportunity to decide how best to protect their citizens when it comes to those companies that have opted out of the federal regulatory scheme.

Procedurally, one large change that would be beneficial toward the effort of passing federal security breach legislation would be creating a right of action in a single entity. The dual authority approach proposed in the Data Security and Breach Notification Act of 2014, while beneficial in that it gives a state's attorney general the authority to enforce its citizens' rights, also increases the amount of potential litigation. By consolidating the authority to bring an action in one entity, such as the Federal Trade Commission, litigation would be reduced while still promoting the rights of United States citizens.

Finally, a law enforcement notification provision, similar to the one proposed in the Data Security and Breach Notification Act of 2014 and The Personal Data Notification & Protection Act, is essential to effective federal security breach legislation. The ultimate goal of any security breach legislation is to minimize the damage experienced by consumers when a data breach occurs. The most effective way to make this happen is to stop security breaches at their source: the hackers who maliciously and illegal attempt to access consumers' "personal information." Federal law enforcement agencies are currently best equipped to track down these hackers and bring them to justice. Therefore, requiring entities that experience a breach to report it to federal law enforcement officials makes sense if the true purpose of passing such federal legislation is to prevent security breaches from happening in the first place.

X. CONCLUSION

Federal security breach legislation has been a Congressional priority for nearly a decade. For the most part, the initiative has received bipartisan support, due to the great costs incurred by both companies and consumers when a breach occurs. Still, no such legislation has been passed. In the meantime, the frequency and cost of security breaches has continued to increase for both companies and consumers. Further, to complicate matters, companies must continue to navigate a complex patchwork of state security breach notification laws, which increase costs and lead to confusion.

While many of the state security breach notification laws are similar, there are several key differences that make compliance difficult for companies that fall victim to a security breach. First and foremost, states differ in what they define as "personal information." Since these

laws are not triggered unless "personal information" has been affected, the company must always determine if any breach, no matter how minor, might trigger even a single state's reporting requirements. In addition, many of the laws differ regarding the timeframe and method of notification once a security breach has occurred. This significantly increases the cost for companies by not only accelerating the timeframe for all reporting, but also by requiring a company to use different mediums depending on the state.

Despite the difficulties and high cost caused by the current state regulatory system, Congress' most recent attempt to pass federal security breach legislation has again failed. Introduced in January 2014, the bill was not able to make it past the Committee on Commerce, Science, and Transportation. Ultimately, the bill contained many of the same hang-ups that had prevented previous federal security breach legislation from passing. Most importantly, Congress has been unable to strike a balance between business interests and consumer advocacy groups regarding the extent to which the legislation should reach. The bill would pre-empt state security breach legislation, causing many consumer advocacy groups to worry that it would not provide as much protection as consumers have been offered under the state regulatory schemes. Businesses interests, on the other hand, are concerned about the increased security requirements the bill would impose.

The proposed federal security breach legislation presented by President Obama to the Federal Trade Commission and discussed during the State of the Union Address takes significant steps toward effective federal legislation in the area. First and foremost, the bill places an emphasis on reporting requirements to law enforcement and federal security agencies. In doing so, the bill would increase the chances that those who perpetrate cyber-attacks are caught and brought to justice. In addition, the elimination of strict security requirements, such as those that would be imposed by the Data Security and Breach Notification Act of 2014, recognizes that there are already sufficient incentives for companies to maintain robust security protection measures and increases the likelihood that businesses would be willing to support the bill.

On the other hand, there are still several concerning areas within the bill that will likely prevent it from passing in its current form. Most importantly, the preemption clause coupled with certain sections of the bill will cause a reduction in protections for consumers within states with the most expansive security breach laws, and possibly for all consumers. Notably, the increase in time allowed to report, and the exclusion of certain types of data currently protected by some states' security breach notification laws, will likely result in strong opposition from consumer advocacy groups in those states and across the nation.

In the end, there are several changes that could be made to current federal security breach legislation that would increase not only the

likelihood that it could be passed, but also its overall effectiveness. First, Congress should eliminate statutory language that imposes preemptive action requirements on behalf of companies to prevent security breaches from occurring. The penalties imposed by such language in the current bill are too harsh and businesses already have a strong incentive to maintain adequate security measures due to the costs, both statutory and reputational, associated with security breaches. Further, businesses lack the technology to keep up with hackers who perpetrate these malicious cyber-attacks, and requiring businesses to attempt to prevent such attacks would likely cause operational costs to skyrocket.

Second, the reporting requirements in the bill should be increased to be at least as strong as the strongest security breach legislation that has been passed by the states. This would guarantee that all consumers were provided protection no matter the state in which they happen to live. In addition, by increasing the reporting requirements, consumer advocacy groups would be more likely to back the preemptive nature of the statute because it would actually increase protections for consumers in most states.

Third, the bill should continue to require that companies that have experienced a security breach report the breach as quickly as possible to federal law enforcement officials. This requirement focuses on the real problem that is occurring, namely the prevalence of cyber-hackers who are committing these malicious attacks on citizen's personal information. As can be seen with the recent cyber-attack on Sony Entertainment, timely reporting to federal law enforcement officials can potentially lead to the identification of the individual or, in the case of Sony, the sovereign nation that perpetrated the attack.[168]

Finally, the bill should include an opt-out requirement that would allow businesses to decide whether to be considered a covered entity under the federal regulatory scheme or continue to exist under the current state regulatory structure. An opt-out provision would allow businesses to perform a cost-benefit analysis comparing the cost of more stringent reporting requirements across the board versus the benefit of uniform reporting requirements. For example, small businesses that operate primarily in a few states with less stringent requirements may wish to opt-out of the federal regulatory scheme due to the increased reporting standards. Further, an opt-out provision would allow states to continue to legislate in the area of data protection for those companies which have opted-out of the federal program. State legislatures, therefore, would still have the freedom to increase their states' standards to greater protect their consumers if they so choose.

Overall, the changes suggested above would increase the likelihood

[168] *See* Williams, *supra* note 118.

of passing federal security breach legislation and increase the effectiveness of any such legislation. The uniform standards imposed by such legislation would save businesses money by allowing them to focus on only one set of reporting requirements. Further, the increased reporting requirements would provide greater protection for consumers across the nation. Finally, by requiring companies that fall victim to a security breach to report it to federal law enforcement officials in a timely manner, the statute would increase the efficiency of investigations and constitute a significant step towards the prevention of cyber-attacks moving forward.

XI. FINAL NOTE

Several significant changes have occurred in relation to federal security breach legislation in 2015. In February 2015, President Obama signed an Executive Order meant to increase the sharing of cyber-threat information.[169] In addition, several bills have been introduced in Congress that are geared towards creating a federal standard for notification in the event of a security breach.[170] Included is a proposed bill that would not contain a "superseding" clause, allowing the states to continue their regulation of security breaches.[171] While some hope that the lack of such a clause may help the legislation get passed,[172] businesses are unlikely to support any federal security breach legislation that does not unify the standards and requirements they must follow. In the meantime, security breaches are becoming increasingly more common, with even the federal government's Office of Personnel Management getting hacked,[173] and lawsuits against businesses continue to pile up.[174] With cybersecurity as a new priority for President Obama's administration, and with information regarding new breaches hitting the news wire almost every day, Congress might, hopefully, finally possess the sense of urgency necessary to pass effective federal security breach legislation.

---

[169] Cameron Kerry, *Privacy and cybersecurity get political legs*, BROOKINGS (Feb. 25, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/02/25-obama-cybersecurity-privacy-summit-kerry.

[170] *See* Katie Nelson, *Should the feds take control over breach notification laws?*, WASHINGTON EXAMINER (July 13, 2015), http://www.washingtonexaminer.com/should-the-feds-take-control-over-breach-notification-laws/article/2567832.

[171] *Id.*

[172] *Id.*

[173] *Id.*

[174] *See* Marianne McGee, *UCLA Faces Lawsuit-Already*, DATA BREACH TODAY (July 22, 2015), http://www.databreachtoday.com/ucla-health-faces-lawsuit-already-a-8427; *see also* Mathew Schwartz, *Will Sony Settle Cyber-Attack Lawsuit?*, DATA BREACH TODAY (June 18, 2015), http://www.databreachtoday.com/blogs/will-sony-settle-cyber-attack-lawsuit-p-1880; *see also* Mathew Schwartz, *Nieman Marcus Lawsuit: Game On, Again*, DATA BREACH TODAY (July 23, 2015), http://www.databreachtoday.com/neiman-marcus-lawsuit-game-on-again-a-8429.